UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/765,390	01/22/2001	Kazue Sako	043034/0164	1020

22428 7590 07/06/2004

FOLEY AND LARDNER
SUITE 500
3000 K STREET NW
WASHINGTON, DC 20007

EXAMINER	
WU, ALLEN S	

ART UNIT	PAPER NUMBER
2135	8

DATE MAILED: 07/06/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

C (Rev. 10/03)

Office Action Summary	Application No.	Applicant(s)	
	09/765,390	SAKO, KAZUE	
	Examiner	Art Unit	
	Allen S. Wu	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 January 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 January 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *3, 6, 7*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-6, 9, 12, 15, and 18-22 are rejected under 35 U.S.C. 102(b) as being anticipated by Ateniese et al (hereinafter Ateniese), "Some Open Issues and New Directions in Group Signatures".

As per claims 1 and 18, Ateniese discloses a participant subsystem (see for example; signer page 207 section 10) that is authorized to anonymously participate in a plurality of sessions using secret information provided by a manager subsystem (see for example; group manager, page 197 section 2) and

a reception subsystem that determines whether it is acceptable for the participant subsystem to participate in a session (see for example; verify, page 207 section 10), wherein

the participant subsystem comprises: an anonymous signing section for authorizing individual data using the secret information depending on session-related information (see for example; one time base g, page 207 section 10) to produce anonymous participation data with anonymous signature (see for example; group signature, page 207 section 10)

and the reception subsystem comprises;

an anonymous signature determining section for determining whether received data its anonymous participation data (see for example; verify, page 207 section 10) with anonymous signature authorized by the participant subsystem; and a sender match determining section for determining whether anonymous signatures of arbitrary two pieces ($V_{1,i,}$, $V_{2,i}$) of anonymous participation data are signed by an identical participant subsystem (see for example; same g must be used, page 207 section 10).

As per claims 2 and 19, Ateniese discloses the claimed limitations as described above (see claim 1). Ateniese further discloses wherein the anonymous signature includes data that is generated by a predetermined expression (see for example; group signature page 205 paragraph 2 and page 207 section 10) using the session-related information and the secret information, wherein the sender match determining section checks the data included in the anonymous signature of received anonymous participation data (see for example; check the uniqueness of ź, page 207 section 10 paragraph 5).

As per claims 3 and 20, Ateniese discloses the claimed limitations as described above (see claim 2). Anteniese further discloses raising a session dependent base (g) to a power that is dependent on the secret information (see for example; page 204 paragraphs 3-4 and page 207 section 10).

As per claim 4, Ateniese discloses the claimed limitations as described above (see claim 1). Ateniese further discloses the anonymous signing section authorizes the individual data based on a group signature scheme (see for example; page 198-199 section 3).

As per claim 5, Ateniese discloses the claimed limitations as described above (see claim 1). As for an escrowed identity scheme, Ateniese further discloses being able to identify the signer by a third party (group manager) and thus an escrowed identity scheme (see for example; OPEN, page 197).

As per claims 6 and 21, Ateniese discloses the claimed limitations as described above (see claim 1). Ateniese further discloses a generator for creating a session-dependent generator depending on the session related information (see for example; trusted entity to generate, page 210 section 10.3);

A group signing section for signing the individual data using the session-dependent generator and the secret information to produce anonymous participation data (see for example; group signature over a message, page 104; and one-time base page 207 section 10), wherein the anonymous participation data includes data obtained by raising the session-dependent generator to a power determined by the secret information (see for example; V_1 := ..., page 204); and

a linkage data generating section for generating linkage data indicating a relationship among the session-dependent generator and a generator determined by the individual data and/or the session related information (see for example; check the uniqueness of ź, page 207 section 10 paragraph 5). Such generator for ź pertaining to the session (one time base) must be present to produce the value.

As per claims 9 and 22, similar limitations are described in claims 6 and 21 above and are rejected under the same rationale.

As per claim 12, Ateniese discloses the claimed limitations as described above (see claim 1). Ateniese further discloses a generator for creating a session-dependent generator depending on the session related information (see for example; trusted entity to generate, page 210 section 10.3);

A escrow identity signing section for signing the individual data using the session-dependent generator and the secret information to produce anonymous participation data (see for example; group signature over a message, page 104; and one-time base page 207 section 10), wherein the anonymous participation data includes data obtained by raising the session-dependent generator to a power determined by the secret information (see for example; V_1 := ..., page 204); and

a linkage data generating section for generating linkage data indicating a relationship among the session-dependent generator and a generator determined by the individual data and/or the session related information (see for example; check the uniqueness of ź, page 207 section 10 paragraph 5). Such generator for ź pertaining to the session (one time base) must be present to produce the value.

Ateniese further discloses that such signing can recover a signors identity by a third part, thus an escrow identity signing section (see for example; OPEN, page 197).

As per claim 15, similar limitations are recited in claim 13 above and are rejected under the same rationale.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-6, 9, 12, 15 and 18-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ramzan et al (hereinafter Ramzan), "Group Blind Digital Signatures:

A Scalable Solution to Electronic Cash", in view of Ateniese et al (hereinafter Ateniese), "Some Open Issues and New Directions in Group Signatures".

As per claims 1 and 18, Ramzan discloses a participant subsystem (see for example; Alice page 57 paragraph 3) that is authorized to anonymously participate in a plurality of sessions using secret information provided by a manager subsystem (see for example; LRF, page 57 paragraphs 3-4) and

a reception subsystem that determines whether it is acceptable for the participant subsystem to participate in a session (see for example; VSF page 58), wherein

the participant subsystem comprises: an anonymous signing section for authorizing individual data using the secret information (see for example; see for example; page 57 Voting section and page 80-81 section A.3.3) to produce anonymous participation data with anonymous signature (see for example; page 57 section Voting and page 80-81 section A.3.3)

and the reception subsystem comprises;

an anonymous signature determining section for determining whether received data is anonymous participation data with anonymous signature authorized by the participant subsystem (see for example; VSR page 58); and a sender match determining section for determining whether anonymous signatures of arbitrary two pieces (V_1 and V_2) of anonymous participation data are signed by an identical participant subsystem (see for example; serial number page 58, and page 80).

Ramzan does not explicitly teach the secret information pertaining being session dependent. Ateniese discloses means of anonymous participation employing group signatures wherein the secret information is session dependent (see for example; page 207 section 10). The base "g" used for producing the signature is used in both Ramzan (see for example; page 80 In 2-4) and Ateniese. However, Ateniese modifies the use of "g" such that it session dependent (see for example; page 207 section 10) such that compositional integrity is upheld for that one-time participating, thus being a valid for one session (see for example; page 206 paragraphs 3-7). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Ateniese within the system of Ramzan because it would have added functionality and compositional integrity.

As per claims 2 and 19, Ramzan-Ateniese discloses the claimed limitations as described above (see claim 1). Ateniese further discloses wherein the anonymous signature includes data that is generated by a predetermined expression (see for example; group signature page 205 paragraph 2 and page 207 section 10) using the session-related information and the secret information, wherein the sender match determining section checks the data included in the anonymous signature of received anonymous participation data (see for example; check the uniqueness of $\acute{z}$, page 207 section 10 paragraph 5).

As per claims 3 and 20, Ramzan-Ateniese discloses the claimed limitations as described above (see claim 2). Anteniese further discloses raising a session dependent base (g) to a power that is dependent on the secret information (see for example; page 204 paragraphs 3-4 and page 207 section 10).

As per claim 4, Ramzan-Ateniese discloses the claimed limitations as described above (see claim 1). Ramzan further discloses the anonymous signing section authorizes the individual data based on a group signature scheme (see for example; group blind digital signatures, abstract).

As per claim 5, Ramzan-Ateniese discloses the claimed limitations as described above (see claim 1). As for an escrowed identity scheme, Ramzan further discloses being able to identify the signer by a third party (group manager) and thus an escrowed identity scheme (see for example; page 81 section A.3.4).

As per claims 6 and 21, Ramzan-Ateniese discloses the claimed limitations as described above (see claim 1). Ramzan further discloses a group signing section for signing the individual data using the secret information to produce anonymous participation data (see for example; pages 80-81 section

A.3.3); and a linkage data generating section for generating linkage data(see for example; serial number pages 57-58).

Ramzan does not explicitly teach a generator creating section for creating a session-dependent generator depending on the session related information and group signing using the session dependent generator and the secret information. Ateniese further discloses such a generator for group signing to produce anonymous participation data, wherein the anonymous participation data includes data obtained by raising the session–dependent generator to a power determined by the secret information (see for example; page 207 section 10) (see for example; page 207 section 10). The common random, one-time base must be generated by some means, thus a session-dependent generator is inherent to the teachings of Ateniese. Ateniese further discloses such session-dependent generator to be used for signing and a linkage data generating section for generating linkage data indicating a relationship among the session-dependent generator and a generator determined by the individual data and/or the session related information (see for example; ź, page 207 section 10 paragraph 5). Such use of session-dependent information allows greater compositional integrity (see for example; Ateniese page 206).t It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Ateniese within the system of Ramzan because it would have added functionality and compositional integrity.

As per claims 9 and 22, Ramzan-Ateniese discloses the claimed limitations as described above (see claim 1). Ramzan further discloses a group signing section for signing the individual data using the secret information to produce anonymous participation data (see for example; pages 80-81 section A.3.3).

Ramzan does not explicitly teach a generator creating section for creating a session-dependent generator depending on the session related information and group signing using the session dependent generator and the secret information. Ateniese further discloses such a generator for group signing to produce anonymous participation data, wherein the anonymous participation data includes data obtained by raising the session–dependent generator to a power determined by the secret information (see for example; page 207 section 10). The common random, one-time base must be generated by some means, thus a session-dependent generator is inherent to the teachings of Ateniese. Such use of session-dependent information allows greater compositional integrity (see for example; Ateniese page 206).t It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Ateniese within the system of Ramzan because it would have added functionality and compositional integrity.

As per claim 12, Ramzan-Ateniese discloses the claimed limitations as described above (see claim 1). Ramzan further discloses an escrow identifying

section for signing the individual data using the secret information to produce anonymous participation data (see for example; pages 80-81 section A.3.3); and a linkage data generating section for generating linkage data(see for example; serial number pages 57-58). Ramzan discloses that the signing can also be identified by a third party, thus an escrow identifying signing (see for example; page 81 section A.3.4)

Ramzan does not explicitly teach a generator creating section for creating a session-dependent generator depending on the session related information and group signing using the session dependent generator and the secret information. Ateniese further discloses such a generator for signing to produce anonymous participation data, wherein the anonymous participation data includes data obtained by raising the session–dependent generator to a power determined by the secret information (see for example; page 207 section 10) The common random, one-time base must be generated by some means, thus a session-dependent generator is inherent to the teachings of Ateniese. Ateniese further discloses such session-dependent generator to be used for signing and a linkage data generating section for generating linkage data indicating a relationship among the session-dependent generator and a generator determined by the individual data and/or the session related information (see for example; ź, page 207 section 10 paragraph 5). Such use of session-dependent information allows greater compositional integrity (see for example; Ateniese page 206). It would have been obvious to one of ordinary skill in the art at the

time of the applicant's invention to combine the teachings of Ateniese within the system of Ramzan because it would have added functionality and compositional integrity.

As per claim 15, similar limitations are recited in claim 13 above and are rejected under the same rationale.

5. Claims 7-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ateniese et al (hereinafter Ateniese), "Some Open Issues and New Directions in Group Signatures" in view of Camenisch et al (hereinafter Camenisch), "Efficient Group Signatures Schemes for Large Groups, and further in view of Grabbe, "Introduction to Digital Cash".

As per claim 7, Ateniese discloses the claimed limitations as described above (see claim 6). Ateniese further discloses a group-signing scheme suggested by Camenisch (see for example; CS97 page 199 and section 10 page 207). Only the "sign" procedure is involves a new initial stage, taking into account a one-time base (see for example; section 10 page 207). As per the secret information being represented by (x,y,v) that satisfies $v=(y+\delta)^{1/e}$, where $y=a^x \bmod n$, n is a product of two prime numbers as used in the RSA cryptography, g is a generator that generates a cyclic group of order n, a is an integer mutually prime to n, e is an integer mutually prime to the Euler number of n, and δ is a constant other than 1, Camenisch discloses such secret information

as part of the join process of basic group signatures (see for example; page 417-417) of which Ateniese relies on.

Ateniese further discloses a session dependent generator g_A corresponding to a session (see for example; section 10 page 207 and section 10.3 page 210; the base "g" is generated),

the group signing section sets $z=g_A^y$ (see for example; page 204) and generates a proof statement

$V_1 = SKLOGLOG(z, g_A, a)[\alpha : z = g_A(a^\alpha)](1)$ (see for example; page 204)

providing the knowledge of a α satisfying $z = g_A^{(a^\alpha)}$ (see for example; x, page 204) and a second proof statement

$V_2 = SKROOTLOG(z * g_A^b, g_A, e)[\beta : z * g_A^b = g_A^{(\beta^e)}](1)$ (see for example V2; page 204)

providing the knowledge of β satisfying $z * g_A^b = g_A^{(\beta^e)}$ (see for example; page 204).

As for a linkage data generating section setting $z_1=g_m^y$ and generating a third proof statement V_3, Ateniese discloses an alternative linking step by generating a third proof statement V_3 (see for example; page 205), however the linkage step is for linking between different groups and not for the generator dependent on individual data g_m. However, Ateniese further discloses that an identity of the person can be found by the group manager (see for example page 197 and page 205). Grabbe further discloses a means of anonymous signature

wherein the notion of "restrictive blind" signature, and the "Schnorr identification scheme" are introduced for privacy protection (see for example; page 3 paragraph 4). Ateniese further suggests a linking in which the group manager is able to identify the signer (see for example page 197). Grabbe further discloses use of a means wherein linkage data is generated (Schnorr identification) such that a user's identity is revealed (see page 3 paragraphs 4-6). Such use of a geometric trap for being able to identify users based on a conditional blinding would have been realized by one of ordinary skill in the art at the time of the applicant's invention and applied to the linkage step of Ateniese. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Grabbe within the Ateniese-Camenisch combination because it would have increased security by prohibiting double voting or additional use of the signature during a session.

As for the anonymous participation data being defined by as (A, M, z, z_1, V_1, V_2, V_3), one of ordinary skill in the art would have recognized such data through the existing data of Ateniese (see for example; page 207 section 10) and the added data of Grabbe (see for example; page 3 paragraph 4).

As per claim 8, Ateniese-Camenisch-Grabbe discloses the claimed limitations as described above. Ateniese further discloses the anonymous signature section checks the anonymous participation data to determine whether received data is anonymous participation data with the anonymous signature

authorized by the participant system (see for example; verify page 207 section 10), and

the sender match determining section checks z of the anonymous participation data to determine whether anonymous signatures of arbitrary two pieces of anonymous participation data are signed by an identical participant system (see for example; duplicate z, page 207 section 10).

6. Claims 10-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ateniese et al (hereinafter Ateniese), "Some Open Issues and New Directions in Group Signatures" in view of Camenisch et al (hereinafter Camenisch), "Efficient Group Signatures Schemes for Large Groups

As per claim 10, Ateniese discloses the claimed limitations as described above (see claim 6). Ateniese further discloses a group-signing scheme suggested by Camenisch (see for example; CS97 page 199 and section 10 page 207). Only the "sign" procedure is involves a new initial stage, taking into account a one-time base (see for example; section 10 page 207). As per the secret information being represented by (x,y,v) that satisfies $v=(y+\delta)^{1/e}$, where $y=a^x \bmod n$, n is a product of two prime numbers as used in the RSA cryptography, g is a generator that generates a cyclic group of order n, a is an integer mutually prime to n, e is an integer mutually prime to the Euler number of n, and δ is a constant other than 1, Camenisch discloses such secret information

as part of the join process of basic group signatures (see for example; page 417-417) of which Ateniese relies on.

Ateniese further discloses a session dependent generator g_A corresponding to a session (see for example; section 10 page 207 and section 10.3 page 210; the base "g" is generated),

the group signing section sets $z=g_A^y$ (see for example; page 204) and generates a proof statement

$V_1 = SKLOGLOG(z, g_A, a)[\alpha : z = g_A(a^\alpha)](1)$ (see for example; page 204)

providing the knowledge of a α satisfying $z = g_A^{(a^\alpha)}$ (see for example; x, page 204) and a second proof statement

$V_2 = SKROOTLOG(z * g_A^{\ b}, g_A, e)[\beta : z * g_A^{\ b} = g_A^{(\beta^e)}](1)$ (see for example V2; page 204)

providing the knowledge of β satisfying $z * g_A^{\ b} = g_A^{(\beta^e)}$ (see for example; page 204).

As for the anonymous participation data being defined by as (A, m, z, z_1, V_1, V_2, V_3), one of ordinary skill in the art would have recognized such data through the existing data of Ateniese (see for example; page 207 section 10).

As per claim 11, Ateniese-Camenisch discloses the claimed limitations as described above. Ateniese further discloses the anonymous signature section checks the anonymous participation data to determine whether received data is

anonymous participation data with the anonymous signature authorized by the participant system (see for example; verify page 207 section 10), and

the sender match determining section checks z of the anonymous participation data to determine whether anonymous signatures of arbitrary two pieces of anonymous participation data are signed by an identical participant system (see for example; duplicate z, page 207 section 10).

7. Claims 13-14 and 16-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ateniese et al (hereinafter Ateniese), "Some Open Issues and New Directions in Group Signatures" in view of Camenisch et al (hereinafter Camenisch), "Efficient Group Signatures Schemes for Large Groups, and further in view of Kilian, "Identity Escrow".

As per claim 13, Ateniese discloses a group signing signature scheme as described above (see claim 12) and further discloses identity escrowing based on the group manager (see for example; Introduction, page 198). However, Kilian suggests that to achieve the a proper identity escrow system, the roles of the issuer and escrow agency must be split (see for example; page 175 paragraph 2).

Ateniese further discloses a session dependent generator g_A corresponding to a session (see for example; section 10 page 207 and section 10.3 page 210; the base "g" is generated),

the escrow identifying section sets z (see for example; page 204). As for generating a first proof statement

$V_1 = SKROOTLOG(z_a, g_A, e)[\alpha : z_a = g_A(a^{\alpha})](1)$ (see for example; page 204)

proving the knowledge satisfying of satisfying $z_a = g_A^{(a^e)}$ (see for example; x, page 204), Ateniese further discloses such generation of a proof statement using SKLOGLOG (see for example; page 204). Ateniese does not explicitly teach the use of SKROOTLOG as in generating a first proof statement. Camenisch further discloses the use SKROOTLOG in place of SKLOGLO for generating proof statements as a more efficient alternative to generating such statements (see for example; page 420 section 6). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to use such SKROOTLOG in place of SKLOGLOG in generation of signatures because it would have provided a means of generating proof statements in a more efficient manner.

As for a second proof statement by setting $z_b = g_A^{(b^e)}$

$V_2 = SKROOTLOG(z_b, g_A, e)[\beta : z_b = g_A^{(b^e)}](1)$ (see for example V2; page 204)

proving the knowledge of β satisfying $z_b = g_A^{(\beta^e)}$ (see for example; page 204), Ateniese discloses a means of generating proof statements for proving the knowledge of α and β respectively (see for example; page 204). Camenisch

further discloses such proof statements generated using SKROOTLOG. Ateniese-Camenisch does not explicitly teach a means of generating secret information being represented by (a,b) that satisfies $b= (a^{e}-\delta)1/e$, mod n, where n is a product of two prim numbers as used in the RSA cryptography, g is a generator that generates a cyclic group of order n, a is an integer mutually prime to n, e is an integer mutually prime to the Euler number of n, and δ is a constant other than 1, Kilian discloses such secret information for creating a separated escrow identity group signature scheme (see for example; page 177 paragraphs 1-2). Ateniese-Camenisch discloses the anonymous group signing as described above see claim 12) and is silent on details of a proper identity escrow system. Kilian further discloses the importance of separating roles of issuing and identity escrowing from the group manager of Ateniese (see for example; page 175 paragraphs 1-2). Ateniese discloses that the first and second proof statements are generated based on a computation of z such that the statements prove the knowledge of secrets respectively (see for example; page 204). Such generation of a first and second proof statements using corresponding generation of z based on such secret information of Kilian would have been realized by one of ordinary skill in the art. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the identity-escrow certificates of Kilian within the Ateniese-Camenisch combination because it would have added the security of a proper identity escrow system to the group signature system of Ateniese-Camenisch.

As for a linkage data generating section setting $z_1=g_m{}^y$ and generating a third proof statement V_3, Ateniese discloses an alternative linking step by generating a third proof statement V_3 (see for example; page 205), however the linkage step is for linking between different groups and not for the generator dependent on individual data g_m. Kilian further discloses a need for some linking based on the identification data of the signer (see for example; page 179 paragraphs 5-7). One of ordinary skill in the art at the time of the applicant's invention would have realized such linkage data generating in creating the third proof statement of Ateniese-Camenisch for the session-dependent data of Ateniese-Camenisch and identification data of Kilian. It would have been obvious to one of ordinary skill in the art to provide such linkage because it would have allowed a higher security by linking an identifier to the session-based signature so as to be able to identify the person by a trusted third party.

As per claim 14, Ateniese-Camenisch-Kilian discloses the claimed limitations as described above. Ateniese further discloses the anonymous signature section checks the anonymous participation data to determine whether received data is anonymous participation data with the anonymous signature authorized by the participant system (see for example; verify page 207 section 10), and

the sender match determining section checks z of the anonymous participation data to determine whether anonymous signatures of arbitrary two

pieces of anonymous participation data are signed by an identical participant system (see for example; duplicate z, page 207 section 10).

As per claim 16, Ateniese discloses a group signing signature scheme as described above (see claim 12) and further discloses identity escrowing based on the group manager (see for example; Introduction, page 198). However, Kilian suggests that to achieve the a proper identity escrow system, the roles of the issuer and escrow agency must be split (see for example; page 175 paragraph 2).

Ateniese further discloses a session dependent generator g_A corresponding to a session (see for example; section 10 page 207 and section 10.3 page 210; the base "g" is generated),

the escrow identifying section sets z (see for example; page 204). As for generating a first proof statement

$V_1 = SKROOTLOG(z_a, g_A, e)[\alpha : z_a = g_A(a^\alpha)](1)$ (see for example; page 204)

proving the knowledge satisfying of satisfying $z_a = g_A^{(a^e)}$ (see for example; x, page 204), Ateniese further discloses such generation of a proof statement using SKLOGLOG (see for example; page 204). Ateniese does not explicitly teach the use of SKROOTLOG as in generating a first proof statement. Camenisch further discloses the use SKROOTLOG in place of SKLOGLO for generating proof statements as a more efficient alternative to generating such statements (see for example; page 420 section 6). It would have been obvious

to one of ordinary skill in the art at the time of the applicant's invention to use such SKROOTLOG in place of SKLOGLOG in generation of signatures because it would have provided a means of generating proof statements in a more efficient manner.

As for a second proof statement by setting $z_b = g_A^{(b^e)}$

$V_2 = SKROOTLOG(z_b, g_A, e)[\beta : z_b = g_A^{(b^e)}](1)$ (see for example V2; page 204)

proving the knowledge of β satisfying $z_b = g_A^{(\beta^e)}$ (see for example; page 204), Ateniese discloses a means of generating proof statements for proving the knowledge of α and β respectively (see for example; page 204). Camenisch further discloses such proof statements generated using SKROOTLOG. Ateniese-Camenisch does not explicitly teach a means of generating secret information being represented by (a,b) that satisfies b= (ae-δ)1/e, mod n, where n is a product of two prim numbers as used in the RSA cryptography, g is a generator that generates a cyclic group of order n, a is an integer mutually prime to n, e is an integer mutually prime to the Euler number of n, and δ is a constant other than 1, Kilian discloses such secret information for creating a separated escrow identity group signature scheme (see for example; page 177 paragraphs 1-2). Ateniese-Camenisch discloses the anonymous group signing as described above see claim 12) and is silent on details of a proper identity escrow system. Kilian further discloses the importance of separating roles of issuing and identity

escrowing from the group manager of Ateniese (see for example; page 175 paragraphs 1-2). Ateniese discloses that the first and second proof statements are generated based on a computation of z such that the statements prove the knowledge of secrets respectively (see for example; page 204). Such generation of a first and second proof statements using corresponding generation of z based on such secret information of Kilian would have been realized by one of ordinary skill in the art. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the identity-escrow certificates of Kilian within the Ateniese-Camenisch combination because it would have added the security of a proper identity escrow system to the group signature system of Ateniese-Camenisch.

As per claim 17, Ateniese-Camenisch-Kilian discloses the claimed limitations as described above. Ateniese further discloses the anonymous signature section checks the anonymous participation data to determine whether received data is anonymous participation data with the anonymous signature authorized by the participant system (see for example; verify page 207 section 10), and

the sender match determining section checks z of the anonymous participation data to determine whether anonymous signatures of arbitrary two pieces of anonymous participation data are signed by an identical participant system (see for example; duplicate z, page 207 section 10).

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Killian et al, US Patent 5,495,532, discloses an anonymous voting system.

Jakobsson et al, US Patent 6,636,969 discloses an anonymous signature system that is traceable.

Franklin et al, US Patent 6,055,518, discloses an anonymous electronic bidding system.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Allen S. Wu whose telephone number is 703-305-0708. The examiner can normally be reached on Monday-Friday 9am-5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AU 2135

Allen Wu
Patent Examiner
Art Unit 2125

ASW